



## Oxygen Forensic Suite – Blackberry IPD backup analysis

### Contents

[About .IPD file](#)

[Methods of Blackberry data extraction](#)

[Two ways of IPD file upload and analysis in Oxygen Forensic Suite 2010](#)

[How Blackberry databases are parsed in Oxygen Forensic Suite 2010 interface](#)

[Databases presentation in Blackberry IPD Viewer](#)

### About .IPD file

Blackberry IPD file (coming from Inter@ctive Pager Backup) is a proprietary backup of the databases on the Blackberry devices. It stores the device information in a binary mode in its own format.

The IPD file is created by the Blackberry Desktop Manager software for Windows OS. It is by default named in the following way:

*Backup-(current date, time and year)-.ipd*

The backup is located by default in the user's **My Documents** folder on PC. Both the file name and the save location can be changed by the user.

Depending on which data was selected for backup, .IPD files may contain anything from the user's address book and emails to memos, SMS messages and even configuration data. But a backup file does not store all the device data because some standard and many third-party applications do not give access to their data.

According to the chosen option backup is either created automatically after the program startup or made by user manually.

Please note that to backup file structure in Blackberry Desktop software version 6 it is necessary to select **Custom backup type** and **Files saved on my built-in media storage** options, like on the screenshot:

Backup type:	
<input type="radio"/>	Full (all device data and settings)
<input type="radio"/>	Quick (exclude email)
<input checked="" type="radio"/>	Custom (selected data only)

Include:	
<input checked="" type="checkbox"/>	Files saved on my built-in media storage

<input checked="" type="checkbox"/> Data Type	Entries
<input checked="" type="checkbox"/> Address Book	3
<input checked="" type="checkbox"/> Address Book - All	3
<input checked="" type="checkbox"/> Address Book - Last Used I	1
<input checked="" type="checkbox"/> Address Book Options	1
<input checked="" type="checkbox"/> Alarm Options	1
<input checked="" type="checkbox"/> Alarms	0

If there is a previous version of Blackberry Desktop Software installed no special options to backup all the data are needed.

After backup process is over two files are created: with .IPD extension and .CAB one. The first file stores all the device data with the exception of file system. The second file contains the information about file



structure of the device and must be put together with .IPD file during backup upload in Oxygen Forensic Suite 2010.

## Methods of Blackberry device extraction

There are two methods of Blackberry device acquisition: physical and logical.

Physical extraction gets a bit-by-bit copy of the entire physical memory using low-level access and special hardware. When speaking about physical acquisition applied to Blackberry devices you should bear in mind the following issue. The data can be encrypted and when a user, for example, adds a contact to the device it is first encrypted and then written into the device internal memory. If a forensic expert uses a physical data extraction he can retrieve encrypted bytes that will not provide him with useful information.

Logical extraction is the extraction of information from the device using various connectivity methods (cables, Bluetooth, Infrared) to retrieve the contents of the phone memory file system.

Oxygen Forensic Suite 2010 is a logical tool and it parses the information from Blackberry device databases (of which .IPD backup is made) and presents it in a readable format. These databases store all the device data and can be parsed in the same way either when you connect a device in Oxygen Forensic Suite 2010 and extract data from it or upload .IPD backup.

## Two ways of IPD file upload and analysis in Oxygen Forensic Suite 2010

There are two ways of .IPD file upload in Oxygen Forensic Suite 2010: loading it in Backup Extraction Wizard or in Blackberry IPD Viewer.

1) To load it in Backup Extraction Wizard press **Load backup file** button on the tool bar. After upload the data will be parsed and presented in phone sections as if you connected a phone and acquired all the data from it.

The screenshot shows the Oxygen Forensic Suite 2010 Analyst interface. The main window displays a list of contacts with columns for Contact, Occupation, Phones, Internet, Addresses, and Private. The contact list includes:

Contact	Occupation	Phones	Internet	Addresses	Private
Abdulrahkim Hashim		General: 03496372 General (home): 981168782340312 Mobile: 7866324907545334123 Fax: 88712768679876432	E-mail: hashim@contactme.com WWW: http://www.taxi.com		Birthda: 16.04.
Abdusalamov Rahim		General (home): 0385046046026 General (office): 0385046046222 Mobile: 044146564	E-mail: abdulalamov@un.org		Note: 6854A
Mr. Adnan John	Company: Undreground cl... Job title: Doctor	General: +837 (0) 318-5548 General (home): +837 (0) 466-5078 General (office): +6738 872024 Mobile: +837 (0) 938-7873 Fax: +957 (87834) 93 Pager: #284746	E-mail: adnan@clinic.ru WWW: http://www.adnandic...	Full address (home): Adenauerplatz, 2 Country (home): Germany Postal code (home): 44983 Region (home): East Germany City (home): Berlin	Note: Glenfid... Birthda: 08.04.
Mrs. Akimicheva E.	Company: Ty-ra Ltd. Job title:	General: 2132312 General (office):	E-mail: kimcheneer@gmail.com	Full address (office): Altybaeva blvd. 19 Country (office):	Note: Drunk ... Birthda: 16.04.

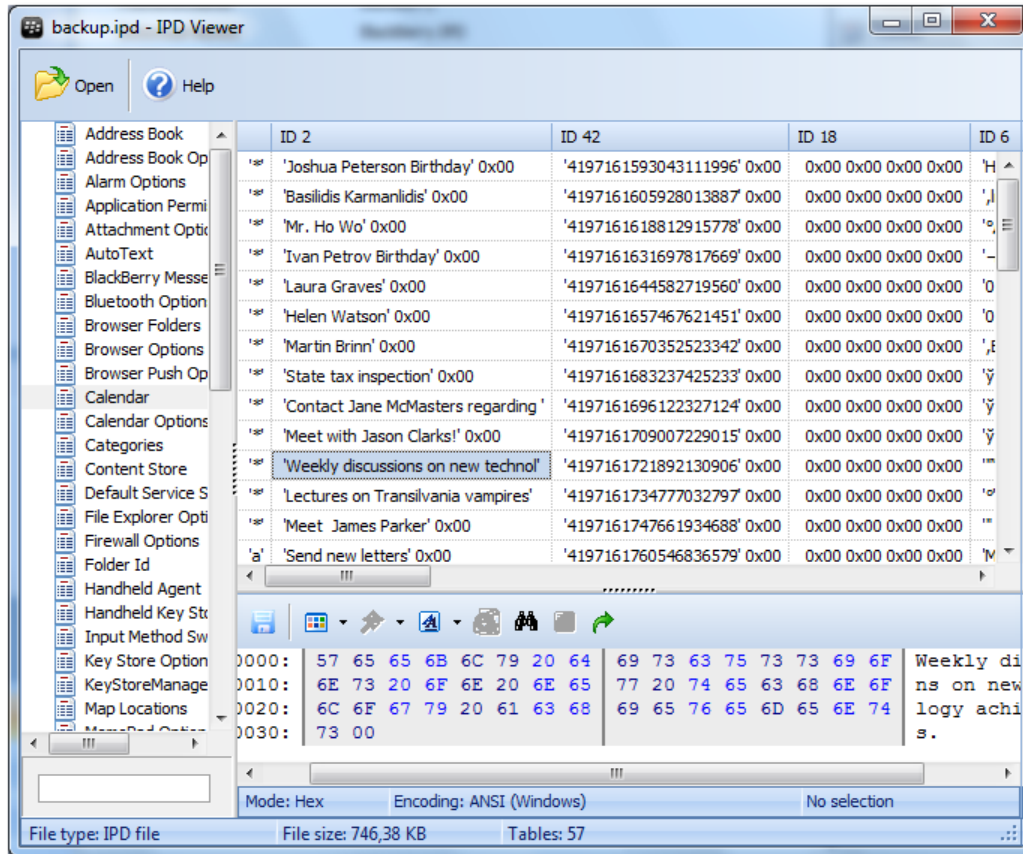
The interface also shows a sidebar with 'Caller groups filter' and 'Contact information' for the selected contact. The status bar at the bottom indicates 'Analyst version: 3.0.0.68', 'Backup-(2010-02-12)-plain\_full', 'Total: 24', 'Filtered: 24', and 'MDS Hash: f9711873f948be81d92ca90635c266b8'.



The great advantage of this way is its clearness: you see all the data in a readable format and you can export it into a variety of reporting formats and, for example, present it in court.

But some specific data, like Bluetooth configuration, message search results, message attachments, etc., saved in .IPD backup will not be shown there.

2) The other way is to upload data with the help of Blackberry IPD Viewer started from **Tools** program menu. As a result, you will get all the .IPD file data in tables. The quantity of tables depends on the amount of data stored in the device.



The second upload method gives you an access to all the data from .IPD file but you have to deal with some raw material presented sometimes in a binary format. So it is more time-taking method but you are able to browse through all the IPD file data.

## How Blackberry device databases are parsed in Oxygen Forensic Suite 2010 interface

If you connect a device in Oxygen Forensic Suite 2010 and extract data from it or load IPD backup with Backup Extraction Wizard you see the following data:

**Phonebook** section contains all the information about contacts: photos, occupation, phones, addresses, notes, birthdays, speed dials, caller groups.

This data is taken from "Address book" and "Address book -all" Blackberry device databases.

**Calendar** section contains all types of events with start/end time, alarm, location and notes data. The data is parsed from "Calendar" and "Calendar -all" Blackberry device databases.

**Tasks** section presents tasks with priority marks and their due date/time.

This information is taken from "Tasks" table of Blackberry device database.

**Notes** section allows to view notes with their titles.

This data is parsed from "Memos" table of Blackberry device database.

**Messages** section makes it possible to analyze SMS, MMS, E-mail messages. Attachments for messages are not supported yet.

To show this data "Messages", "Saved E-mail Messages" and "SMS Messages" database tables are parsed.



**Event Log** section shows incoming, outgoing and missed calls with duration, time stamp and remote party.

This data is taken from "Phone Call Logs" table of Blackberry device database.

**File Browser** section permits to inspect Blackberry file system, including photos, videos, voice records, documents, etc.

Cab file is parsed to show the information about files stored in Blackberry devices.

## Databases presentation in Blackberry IPD Viewer

Press **Load backup file** button on the toolbar and you will get Blackberry device databases presented in tables. The quantity of tables depends on the options chosen during backup.

Each table usually stores the data of one application. The format and the number of databases depend on the OS version. The quantity of fields in each entry is not fixed so various entries of one table may contain various quantity of fields (sometimes even several fields of the same type for one entry).

Each field contains its ID and the data itself in a set of bytes.

Here is a description of forensically interesting databases:

**Address book** table contains the fullest information about contacts: names, nicknames, occupation, picture, numbers, addresses, birthdays, notes, web pages, etc.

ID 32	ID 33	ID 77	ID 1	ID 42	ID 7
'Abdul' 0x00	'Private Military Servic...	<Jpeg image>	'mahmuddi@abdullah.co...	'Brigade Genera...	'982341238732' 0x00
'Ahmed' 0x00	'Private Military Servic...	<Jpeg image>	'ahmedmurtaza@pmc-pm...	'Brigade Officer'...	' +234987328798798' 0x00
'Andre' 0x00	'New Inventions Foun...	<Jpeg image>	'dujardin@andre.com' 0x00	'Coordinator' 0x00	

Each row of the table belongs to one contact. If a cell is grey it means this cell does not exist in the backup. Pressing on Jpeg image opens a contact photo below in a Hex viewer.

The fields are parsed in the following way:

<i>ID</i>	<i>Description</i>
32	FirstName
160	FirstName
55	Title
183	Title
33	Company
161	Company
77	Picture
42	Job
170	Job
6	Phone Work
16	Phone Work 2
7	Phone Home
17	Phone Home 2
8	Phone mobile
19	Phone mobile 2
9	Pager
3	Fax
20	Home Fax
18	Phone Other
10	Pin
35	Work address 1
163	Work address 1
36	Work address 2



164	Work address 2
38	Work city
166	Work city
39	Work state
167	Work state
40	Work ZIP
41	Work country
169	Work country
61	Home address 1
189	Home address 1
62	Home address 2
190	Home address 2
69	Home city
197	Home city
70	Home state
198	Home state
71	Home ZIP
72	Home country
200	Home country
82	Birthday
83	Anniversary
59	Categories
54	Web page
65	User 1
66	User 2
194	User 2
67	User 3
195	User 3
68	User 4
196	User 4
64	Notes
192	Notes
86	NickName
214	Nickname

**Address book –all** table reflects the total number of add up contact list entries for multiple contact lists. All the contact fields are packed in one cell with ID 10.

ID 2	ID 3	ID 5	ID 10
'яяяяяяяя'	'?? ?????????'	'ф' 0x1A'±-'	0x06 0x00' Zyxel' 0x00'o' 0x0A'МяШяб' 0x01'ZExif' 0x00 0x00'II'±' 0x00 0x08 0x00 0x00 0x00 0x00

**Quick contacts** table stores phone numbers in a Speed Dial list.

ID 1	ID 31	ID 2	ID 10	ID 13	ID 11	ID 12
'; 0x12'46'...	'Bruno' 0x00	'P' 0x00	0x00 0x00 0x00 0x00 0x0...	0x02 0x00 0x00 0x00	0x01 0x00 0x00 0x00	'3650834' 0x00
'; 0x12'46'...	0x00	'W' 0x00	0x00 0x00 0x00 0x00 0x0...	0x00 0x00 0x00 0x00	0x00 0x00 0x00 0x00	0x00

The fields are parsed in the following way:

<i>ID</i>	<i>Description</i>
2	SpeedKey
12	Phone number



- 31        FirstName, LastName
- 159      FirstName, LastName
- 55        Title
- 183      Title

**Phone HotList** table stores information on the last x# of calls placed from the BlackBerry smartphone.

	ID 31	ID 11	ID 12	ID 2	ID 4
'h'	0x00	0x00 0x00 0x00 0x00	'89630411041' 0x00	0x01 0x00 0x00 0x00	0x00'\&' 0x05 0x00 0x00 0
'h'	0x00	0x00 0x00 0x00 0x00	'89060356956' 0x00	0x02 0x00 0x00 0x00	0x00'\&' 0x05 0x00 0x00 0
'h'	'Arnold Polgar' 0x00	0x03 0x00 0x00 0x00	'89035841186' 0x00	0x03 0x00 0x00 0x00	0x00'\&' 0x05 0x00 0x00 0

The fields are parsed in the following way:

- ID*        *Description*
- 2        Whole Duration
- 3        Last call timestamp
- 11       Last call duration
- 12       Last phone number
- 31       Display Name
- 159      Display name

**Phone Call Logs** table presents calls history.

	ID 11	ID 31	ID 12	ID 13	ID 4
'p'	0x00 0x00 0x00 0x00	0x00	'+79038540000' 0x00	0x03 0x00 0x00 0x00	'Ф' 0x1F 0x10'&' 0x01 0x00 0x00
'p'	0x03 0x00 0x00 0x00	'Arnold Polgar' 0x00	'89035841186' 0x00	0x00 0x00 0x00 0x00	'А4уъ&' 0x01 0x00 0x00
'p'	0x03 0x00 0x00 0x00	'Arnold Polgar' 0x00	'89035841186' 0x00	0x00 0x00 0x00 0x00	'о' 0x09'«&' 0x01 0x00 0x00

The fields are parsed in the following way:

- ID*        *Description*
- 2        Call status
- 3        Call duration
- 4        Call timestamp
- 8        Call note
- 12       Phone number
- 31       Display name
- 159      Display name
- 183      Title

**Calendar** table shows calendar events data.

ID 28	ID 40	ID 4	ID 3	ID 27
0x00	0x00	'Second Directorate' 0x00	'Mr. J. Kingsley. Office 222334' 0x00	0x0C 0x00 0x00 0x00 0x01 0x00 0x00
0x00	0x00	'Office N 136234' 0x00	'1.' 0x09'Transfer 1000000\$ and 545000 E'	0x0C 0x00 0x00 0x00 0x01 0x00 0x00
0x00	0x00	'Office N 136234' 0x00	'1.' 0x09'Transfer 1000000\$ and 545000 E'	0x0C 0x00 0x00 0x00 0x01 0x00 0x00

The fields are parsed in the following way:

- ID*        *Description*



- 2 Subject
- 130 Subject
- 3 \*
- 131 \*
- 4 Location
- 132 Location
- 6 Start timestamp
- 7 End timestamp
- 28 IsInStatus
- 40 Public

\* means that a field contains multiline text.

**Calendar –all** table contains the total number of add up entries for all calendars. All the event fields are packed in one cell with ID 10.

ID 2	ID 3	ID 5	ID 10
'ZbTNZbTN'	' ? Groups'	'a1.s'	0x01 0x00 0x01'a' 0x0B 0x00 0x04'Basketball' 0x00 0x14 0x00'*829962544931'

**Memos** table contains memos with their title and details.

...	ID 129	ID 130
'm'	0x01 0x04'' 0x04'5' 0x04'A' 0x04'B'	0x01 0x04'' 0x04'5' 0x04'A' 0x04'B' 0x00'' 0x04'@' 0x04'C' 0x04'A' 0x04'A' 0x04:' 0x04'8' 0x04'B'

The fields are parsed in the following way:

- | <i>ID</i> | <i>Description</i> |
|-----------|--------------------|
| 1         | Title              |
| 129       | Title              |
| 2         | Details            |
| 130       | Details            |

**Tasks** section shows a list of tasks with their parameters.

	ID 130	ID 9	ID 10	ID 16	ID 6	ID 8
't'	0x01 0x04 0x17 0x04'0' 0x04'4...	0x01 0x00 0x00 0x00	0x02 0x00 0x00 0x00	;' 0x00 0x00 0x00	'дГ' 0x03	0x01 0x00 0x00

The fields are parsed in the following way:

- | <i>ID</i> | <i>Description</i>   |
|-----------|----------------------|
| 2         | Task title           |
| 130       | Task title           |
| 3         | Note                 |
| 131       | Note                 |
| 16        | TimeZone             |
| 9         | Status *             |
| 8         | Due                  |
| 14        | Priority **          |
| 17        | Categories list      |
| 6         | Due to timestamp     |
| 15        | Reminder timestamp   |
| 5         | Recurrence timestamp |

\*



Status 0 - Not started, 1 - In progress, 2 - Completed, 3 - Waiting, 4 - Deferred

\*\*

Priority 0 - Low, 1 - Normal, 2 - High

**Saved E-mail messages** section stores saved E-mail messages.

ID 0	ID 100	ID 75	ID 1	ID 2	ID 11	ID 12
0x00 0x00'b' 0x00...	0x08 0x00 0x0...	'~' 0x15'ÿ&'	'яяя' 0x01'я' 0x00 0x01 0x...	'яяя' 0x0...	'Hello' 0x00	'Hey dude' 0x00
0x00 0x00'a' 0x00...	0x08 0x00 0x0...	'~' 0x15'ÿ&'	'яяя' 0x01'я' 0x00 0x01 0x...	'яяя' 0x0...	'Hello' 0x00	'Hey dude' 0x00

The fields are parsed in the following way:

ID	Description
1	Recipients List
5	Sender
6	ReplyTo
11	Subject
139	Subject
24	Message Body
2	FCC list
12	Email Text
140	Email text

**Messages** section stores all the messages on the BlackBerry smartphone.

ID 100	ID 75	ID 11	ID 12	ID 1	ID 2
0x08 0x00 0x00 0x00	'~' 0x15'ÿ&'	'Hello' 0x00	'Hey dude' 0x00	'яяя' 0x01'я' 0x00 0x01 0x03 0x00'hfdkv' 0x00	'яяя' 0x01'я' 0x00 0
0x08 0x00 0x00 0x00	'~' 0x15'ÿ&'	'Hello' 0x00	'Hey dude' 0x00	'яяя' 0x01'я' 0x00 0x01 0x03 0x00'hfdkv' 0x00	'яяя' 0x01'я' 0x00 0

The fields are parsed in the following way:

ID	Description
1	Recipients List
5	Sender
6	ReplyTo
11	Subject
139	Subject
24	Message Body
2	FCC list
12	Email Text
140	Email text

**SMS messages** section contains all SMS messages.

ID 4	ID 1	ID 9	ID 11	ID 2	ID 7
'Hello mama. I am in Finland.'	0x00' ' 0x00...	0x01 0x00 0x00...	0x00 0x00 0...	0x00 0x00 0x00 ...	0x00 0x00 0x0...

The fields are parsed in the following way:

ID	Description
1	Direction, sent timestamp, received timestamp *



- 2 Number
- 4 Text
- 7 Is Unicode\*\*

\*  
The first byte denotes direction: 0 stands for incoming, 1 means outgoing.  
\*\*

If the first byte equals 2 it is a Unicode message.

**Browser Bookmarks** section contains bookmarks for web pages in the browser applications.

ID 18	ID 17
0x00'ghttp://www.t-mobile-favourites.'	'-3N9q' 0x00 0x04 0x01 0x00 0x00F'P'PsPj. СГС,СЪ.ГЯЯЯШРЯ'
0x00'hhttp://www.t-mobile-favourites.'	'-3N9p' 0x00 0x04 0x01 0x00 0x00F'P'PsPj. СГС,СЪ.ГН9ьШЦВг-к'
0x00 0x15'http://www.gazeta.ru/' 0x01'B' 0x00 0x00 0x00 0x00 0x...	'-3Bh' 0x01 0x04 0x01 0x00'8P'P'P-PC,P°,Ru вЪ" P" P'

The fields are parsed in the following way:

- ID Description
- 17 Title
- 18 URL

**Searches** section contains the settings configured in search application.

	ID 1	ID 2	ID 7	ID 10
'f	'Incoming' 0x00	'i' 0x00	0x01 0x00 0x00 0x00	
'f	'Outgoing' 0x00	'o' 0x00	0x02 0x00 0x00 0x00	
'f	'Phone Calls' 0x00	'p' 0x00		0x03 0x00 0x00 0x00
'f	'SMS Messages' 0x00	's' 0x00		0x02 0x00 0x00 0x00

The fields are parsed in the following way:

- ID Description
- 1 Name
- 129 Name
- 2 Hotkey
- 4 Message theme
- 132 Message theme
- 5 Contact name
- 133 Contact name
- 6 SearchIn \*
- 7 Message status \*\*
- 8 Search In directory
- 10 Message type \*\*\*
- 14 Id1
- 15 ID2
- 16 Include encrypted message \*\*\*\*

\*  
SearchIn = 8 – search in BCC, 7 –search in CC, 6 –search in To, 4- search in From, 5 – search in any.

\*\*  
Message status = 5 - Unopened, 4 - Draft, 3 - Saved, 2 - Sent, 1 – Received.  
\*\*\*



Type = 9 – E-mail with attachment, 8 - Pin, 5 – Voice Mail, 3 - Phone calls, 2 - SMS, 1 – E-mail.  
\*\*\*\*

Include encrypted message = 3 otherwise false.

**Bluetooth options** section stores Bluetooth settings.

ID 0	ID 1	ID 2	ID 5	ID 6	ID 7
0x02 0x00 0x0...	'BlackBerry 8800'	0x06 0x00 0x00 0x0C'h' 0x04 0x...	0x17\T#'	0x00 0x00 0x00 0x00	0x01 0x00 0x00 0x00

The fields are parsed in the following way:

ID	Description
0	Discovery options*
1	Device Name
2	Paired Device**
10	Device ID MAC
6	Allow outgoing calls
7	Address Book ***

\*

If Discovery options = 1, then Discoverable - False, Led Indicator – True;

If Discovery options = 3, then Discoverable - True, Led Indicator – True;

If Discovery options = 5, then Discoverable - False, Led Indicator – False;

If Discovery options = 7, then Discoverable - True, Led Indicator – False.

\*\*

Paired Device field stores a packed list of bonded Bluetooth devices.

\*\*\*

Address Book = 0 - Disable, 1 - All entries, 2 - Hot list, 3 - Selected category only.